Security Architecture Documentation Guidance

Version 0.2

Prepared by HR CDS TT

23 June 2011

REVISION HISTORY

Name	Date	Reason For Changes	Version
HRCDSTT	22 June 2011	Initial Review Draft	0.1
	23 June 2011	Updated Draft	0.2

ACRONYMS AND DEFINITIONS

Acronym	Definition
CCA	Covert Channel Analysis
CDS	Cross Domain Solution
DRD	Development Representation Documentation
DTLS	Descriptive Top-Level Specification
FTLS	Formal Top-Level Specification
HLD	High Level Design
LLD	Low Level Design
SP	Security Policy
UCDMO	Unified Cross Domain Management Office

INTRODUCTION

The Security Architecture document provides a high-level introductory presentation of the system security design, in sufficient detail that the security architecture, its major structural units, and its associated security policy can be understood.

The content of the Security Architecture document provides evidence contributing to the level of robustness of the system, how this robustness is achieved, and the system security principles, subsystems, mechanisms and policies which provide the basis for this robustness.

The Security Architecture document lays the foundation for establishing assurance in the system by:

- defining the system's philosophy of protection,
- providing a graphical representation of the system architecture (an architectural diagram),
- providing a description of the characteristics of each subsystem of the system security architecture (its function, its place in the architectural decomposition, its relationship to other architectural subsystems), and
- describing how the fundamental security principles (e.g., domain separation, process isolation, resource encapsulation, modularity, simplicity, least privilege) are realized by the system security architecture.

The Security Architecture document provides interested parties (e.g., consumers, data owners, evaluators, developers) with a first step towards assessing the completeness and correctness of the system design and implementation, thus contributing towards establishing a level of assurance.

A good rule of thumb is that the level of detail of the system Security Architecture document should allow an individual with a degree in Computer Science or Electrical/Computer Engineering with knowledge and skills in software, hardware, or firmware development to understand the system in sufficient detail to understand how changes to the system could affect the robustness of the system.

Figure 1 (next page) depicts the relationship of the Security Architecture document to other security documents defined in the DRD. The Security Architecture document should show that the system security architecture is sufficient to satisfy the system security objectives. Analysis should show that the security architecture is correctly reflected in the system functional specification and the system high level design.

GOAL OF THE SECURITY ARCHITECTURE DOCUMENT

The Security Architecture document is intended to show that the system security objectives are completely and accurately refined into the system security architecture. The system security architecture influences the security design of the system by being refined into the system Security Functional Specification and the system High Level Design.

The Security Architecture document must provide enough detail to enable an experienced security designer or evaluator to understand the system security boundary, the subsystems that comprise the

system security architecture, the security relevance of each subsystem, and the major protection mechanisms on which system assurance is established.

DISCUSSION / GUIDANCE

Philosophy of Protection

The Security Architecture document begins by presenting the system's philosophy of protection. The philosophy of protection presents a high-level, natural-language description of the system security mechanisms and their relationship to the system security policy. The description of the philosophy of protection should demonstrate how the philosophy is derived from and is sufficient to satisfy the system security objectives and the system security requirements.

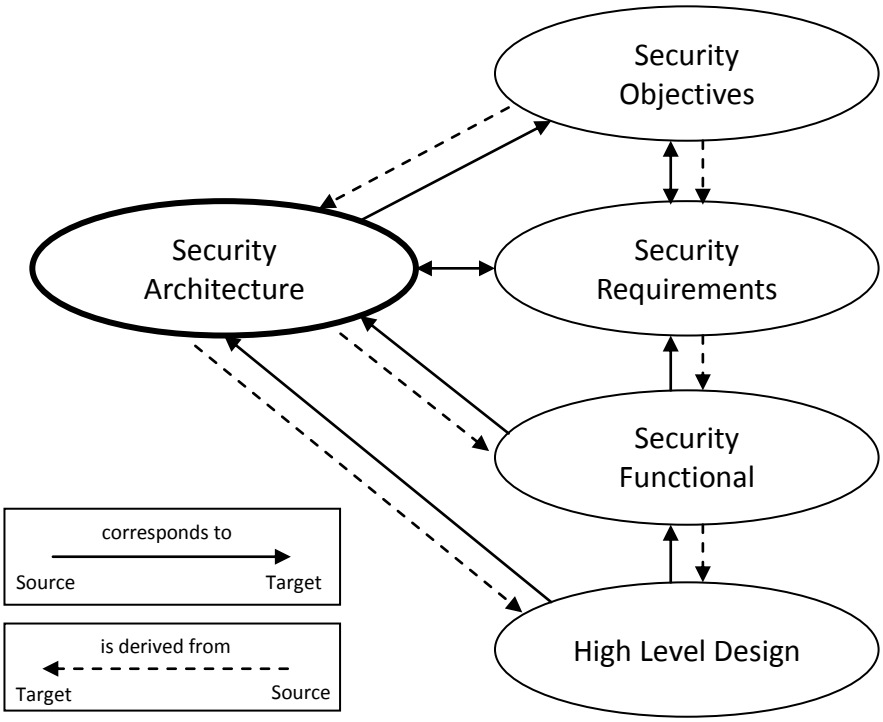

Figure 1 – Security Architecture Interrelationships

Security Architecture Diagram

The Security Architecture document must also provide a decomposition of the system into major subsystems while defining their hierarchial relationships and dependencies, typically starting with a single page architectural diagram[1][2] and then descriptive content explaining the subsystems of the

[1] **It can be asserted that the inability of the system developer to provide a single page architectural diagram that clearly identifies the major subsystems of the system, their relationships, and security relevance is an indication that the system does not meet the high robustness principle of being "conceptually simple".**

[2] **The single page diagram can be further decomposed into additional, more detailed diagrams for each major architectural component. The control and data flows between components can be provided in these more detailed diagrams.**

architectural diagram in detail. A simple, notional example of an architectural diagram is included in Figure 2. An actual architectural diagram of a real system would be expected to be much more detailed and more specific in identifying architectural subsystems.

The security architectural diagram shall:

- Include all major functional subsystems of the system
- Show the subsystems that interact directly with platform hardware
- Depict the layering of the system subsystems
- Represent dependencies among subsystems
- Represent dependencies on external entities

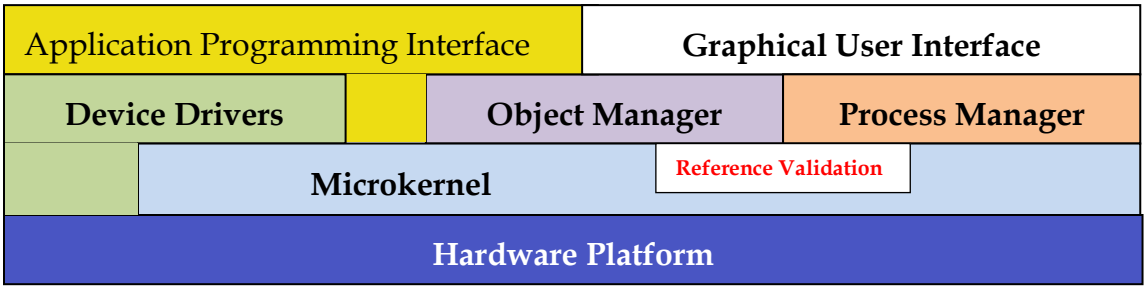

Figure 2 – Example Security Architecture Diagram

Security Architecture Description

The architectural diagram must be accompanied by text descriptions which provide details of each of the major subsystems of the architecture, their security roles and relevance, and their relationships to each other.

Security Architecture Mechanisms

The Security Architecture document provides a description of the fundamental security mechanisms that allow the system to:

- protect itself from untrusted entities (users, application, other systems subsystems and programs),
- separate untrusted entities from each other, and
- control the actions of entities to ensure that the system security policy is enforced.

Implementation of Security Principles

Finally, the Security Architecture document presents, for each of the following fundamental security principles, an argument as to how the principle is realized in the system security architecture. This description should include brief explanations of the mechanisms employed (e.g., virtual memory management, processor states, privilege mechanisms) and how they are used in implementing the security principles.

Because many of these principles do not provide interfaces that allow for direct testing, only analysis of the design and implementation can provide assurance in their completeness and correctness. Thus, the importance of the system design documentation, beginning with the Security Architecture document, is crucial to establishing system robustness.

- Domain separation
- Process isolation
- Resource encapsulation
- Modularity
- Simplicity
- Least privilege
- Secure Initialization, Safe Failure, and Trusted Recovery

REQUIREMENTS

ARC-1 The developer shall provide a system Security Architecture document.

ARC-2 The Security Architecture document shall provide a description of the system philosophy of protection.

ARC-3 The Security Architecture document shall provide a security architectural diagram of the system.

ARC-4 The security architectural diagram shall include all the major subsystems of the system and shall indicate their security relevance (security enforcing, security supporting, security non-interfering), their relative position in the system architecture (peer subsystems, layered subsystems), and their relationships and dependencies.

ARC-5 The developer shall provide a description of the security architecture of the system. This description should correspond to the security architectural diagram.

ARC-6 The security architecture description shall describe the function and role of each subsystem in the security architecture and the inter-relationships between the subsystems, to include dependencies and control and data flows.

ARC-7 The security architecture shall describe how the system protects itself from corruption by untrusted entities.

ARC-8 The security architecture shall present an argument that all references to controlled data and resources (information flows) are mediated by the system security mechanisms.

ARC-9 The security architecture shall present an argument that the system security architecture is logically structured and small enough to be understood and analyzed.

ARC-10 The Security Architecture document shall describe the domain separation mechanisms that provide protection for the system from the untrusted domain.

ARC-11 The Security Architecture document shall describe the process isolation mechanisms that maintain separation between entities.

ARC-12 The Security Architecture document shall describe the resource encapsulation mechanisms that allow for complete mediation of all access to protected resources.

ARC-13 The Security Architecture document shall show that the system security architecture is organized in a modular fashion.

ARC-14 The Security Architecture document shall present an argument as to how the security architecture supports a modular design and implementation.

ARC-15 The Security Architecture document shall present an argument that the system security architecture is conceptually simple.

ARC-16 The Security Architecture document shall describe how the system security architecture is structured to implement the principle of least privilege.

ARC-17 The Security Architecture document shall describe the process and mechanisms related to secure system initialization, safe failure and trusted recovery.